

**Method for control of processing of objects or access control lists for data processing systems, based of defined rules that depend on the type of object and processing events it relates to**

**Patent number:** DE10152121  
**Publication date:** 2003-05-08  
**Inventor:** MOERL RAMON (DE); KOKE ANDREAS (DE);  
HARTMANN PETER (DE)  
**Applicant:** SIOS GMBH FUER DV ARCHITEKTURE (DE)  
**Classification:**  
- **international:** G06F12/14  
- **european:** G06F21/00N9A2; H04L29/06C6C  
**Application number:** DE20011052121 20011023  
**Priority number(s):** DE20011052121 20011023

**Report a data error here**

**Abstract of DE10152121**

Method has the following steps: generation of a control request by an access device when an event is detected that relates to an object, whereby the control request includes event and object describing information; transfer of the control request to a control device; selection of a processing rule for the object based on the included event and object information; and processing of the object according to the processing rule. The invention also relates to a corresponding computer program product and device for implementation of the method.

---

Data supplied from the **esp@cenet** database - Worldwide

**THIS PAGE BLANK (USPTO)**



①⑨ BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENT- UND  
MARKENAMT

⑫ **Offenlegungsschrift**  
⑩ **DE 101 52 121 A 1**

⑤① Int. Cl.<sup>7</sup>:  
**G 06 F 12/14**

②① Aktenzeichen: 101 52 121.9  
②② Anmeldetag: 23. 10. 2001  
④③ Offenlegungstag: 8. 5. 2003

DE 101 52 121 A 1

⑦① Anmelder:  
SIOS GMBH für DV-Architekturen, 81247 München,  
DE  
  
⑦④ Vertreter:  
HOFFMANN · EITLE, 81925 München

⑦② Erfinder:  
Mörl, Ramon, 81247 München, DE; Koke, Andreas,  
85659 Forstern, DE; Hartmann, Peter, Prof. Dr.,  
82223 Eichenau, DE  
  
⑤⑥ Entgegenhaltungen:  
WO 99 30 217

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

Prüfungsantrag gem. § 44 PatG ist gestellt

⑤④ Regelbasierte Verarbeitungskontrolle mobiler Information

⑤⑦ Regelbasierte Verarbeitungskontrolle mobiler Information für eine dezentrale regelbasierte Verarbeitungskontrolle von Objekten, die in ein DV-Gerät importiert oder exportiert werden sollen oder dort verwendet werden sollen. Eine Kontrollanfrage wird durch eine Zugriffsvorrichtung bei Erfassung eines Ereignisses im Zusammenhang mit einem Objekt erzeugt und an eine Steuervorrichtung übertragen. Dort wird eine Verarbeitungsvorschrift für das Objekt aufgrund von Ereignisinformation und Objektinformation ausgewählt und das Objekt wird entsprechend der ausgewählten Verarbeitungsvorschrift verarbeitet.

DE 101 52 121 A 1

## Beschreibung

## Gebiet der Erfindung

[0001] Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Durchführung einer Verarbeitungskontrolle auf Objekte in einem DV-Gerät oder auf Objekte mit einer Repräsentation in einem DV-Gerät, sowie auf Objekte bzw. deren Repräsentationen, welche in ein oder aus einem DV-Gerät übertragen werden sollen.

## Hintergrund der Erfindung

[0002] Zugriffskontrollverfahren sind in der Informationstechnik bekannt und werden eingesetzt, wie beispielsweise beschrieben in O. Fries u. a., Sicherheitsmechanismen, Oldenbourg 1993, H. Kersten, Sicherheit in der Informationstechnik, Oldenbourg 1995, S. Garfinkel, G. Spafford, Practical Unix & Internet Security, O'Reilly 1996, A. D. Rubin u. a., Web Security Sourcebook, Wiley Computer Publishing, 1997, und D. B. Chapman u. a., Einrichten von Internet Firewalls, O'Reilly 1997.

[0003] Dabei treten stets Subjekte, Objekte und Methoden auf: Ein Subjekt möchte mit einer Methode auf ein Objekt zugreifen. Nach verschiedenen Verfahren wird dieser Wunsch gewährt oder verweigert. Zugriffsschutzmodelle teilen sich ein in die beiden Haupttypen

- benutzerbestimmte Zugriffskontrolle (DAC, discretionary access control)
- regelbasierte Zugriffskontrolle (MAC, mandatory access control)

[0004] Die Zugriffsschutzinformation wird dabei entweder in einer Zugriffsschutzmatrix gehalten, oder als Attribut an die Subjekte (Gruppen, Rollen, Privilegien) bzw. an die Objekte (Access Control Lists) gebunden. Auch Kombinationen dieser Verfahren sind üblich und in Produkten vorhanden. Das Erstellen der Zugriffsschutzmatrix erfordert für jedes Paar Subjekt/Objekt einen administrativen Vorgang, ebenso das Anhängen von Attributen an Subjekte bzw. an Objekte.

[0005] Ein wesentliches administratives Problem besteht darin, neu in das System eingeführte Objekte automatisch mit der richtigen Zugriffsschutzinformation zu versehen. Mehrere Verfahren sind hierzu bekannt: Wird ein Objekt von der Administration in ein System importiert, so ist eine regelbasierte Zugriffskontrolle möglich:

- das Vererbungsverfahren: Dabei erben Objekte die Zugriffsschutzinformation von dem schon vorhandenen Container, in dem sie gelagert werden (z. B. Unix, Windows NT/2000).
- Objektklassifizierung: Objekte werden in Typen eingeteilt (z. B. an Hand der Dateierweiterung) und davon abhängig die Zugriffsschutzinformation erzeugt.

[0006] In verteilten Systemen sind die Subjekte häufig Computerbenutzer, die Objekte in ihren Rechner importieren wollen. Solche Objekte sind dann im Besitz des Benutzers, der selbst die Verarbeitungsregeln für das Objekt bestimmt. Hierzu sind DAC-Methoden bekannt:

- Einbringen in einen Container und Zuordnung von Rechten entsprechend dem Vererbungsverfahren.
- Neu einzuführende Objekte werden mit Hilfe einer digitalen Unterschrift signiert. An Hand der Signatur, die den Erzeuger des Objektes identifiziert, wird dem

Subjekt die Entscheidung über eine Verwendung überlassen. (z. B. in ActiveX realisiert).

- Aus der Internettechnologie ist das Prinzip der Sandbox bekannt, in dem aktive Objekte die in das System eingeführt werden nur begrenzte Rechte erhalten, und somit nur begrenzte Verwendung möglich ist.

- In Firewall Systemen werden "Application Proxies" als Filter eingesetzt, die für Internet Anwendungen applikationsspezifisch den Durchgang von Daten erlauben oder verweigern.

[0007] Ein weiteres administratives Problem bei verteilten Systemen besteht darin, dass beim Empfänger eines Objektes vor dem Zugriff dessen Integrität garantiert werden muss. Die Integrität von Objekten kann mit Hilfe einer digitalen Signatur gewährleistet werden.

[0008] In modernen DV-Systemen ergibt sich aus verschiedenen Faktoren, die Notwendigkeit eines neuartigen Sicherheitssystems das durch die existierenden Zugriffsschutzverfahren nicht geleistet werden kann: Es wird immer mehr in Netzwerken gearbeitet, die zentral administriert werden, wobei die Endbenutzer von administrativer Tätigkeit entlastet werden. Diese Entlastung bedeutet beispielsweise die automatisierte Aktivierung von Vorgängen, wie etwa der Installation von Software ohne Einfluss und Kontrollmöglichkeit durch den Anwender.

[0009] Hohe Datenvolumina, große Benutzergruppen und die komplexe Struktur von Anwendungen und Nutzdaten verhindern häufig eine direkte Kontrolle der Administration darüber, dass mit Objekten auf den DV-Geräten so verfahren wird wie vorgeschrieben oder beabsichtigt. Software kann beispielsweise direkt von externen Providern an Endanwender geliefert und von diesen installiert werden.

[0010] Dabei sind die Rechner der Endbenutzer teils stets im Netzwerk eingebunden, werden teils aber auch netzunabhängig betrieben oder nur gelegentlich über, Infrarot oder andere Schnittstellen an das Netz angebunden.

[0011] Konsequenzen dieser Netz- und Verwaltungsstruktur sind zum Beispiel:

- Ein DV-Gerät kann Anwendungen (auch sicherheitsrelevante) von einer unbekannten Netzquelle über nicht vertrauenswürdige Transportwege zur Verfügung gestellt bekommen. Dies kann sogar ohne Kenntnisnahme eines Benutzers geschehen.
- Eine Kommunikationsverbindung zu einem DV-Gerät kann automatisch aufgebaut werden und ein Datenaustausch kann stattfinden, ohne dass dieser vom Besitzer der Information initiiert wurde oder diesem Besitzer überhaupt bekannt ist.

[0012] Die einfache und notwendige Zielsetzung, auf einem DV-Endgerät oder in einem DV-System zu jedem Zeitpunkt die Kontrolle zu haben, welcher Softwarestand, in welcher Konfiguration auf welchen Daten benutzt werden darf, und mit welchen Verfahren auf welche - möglicherweise noch unbekannten - Daten der Benutzer welche Zugriffsrechte besitzt, lässt sich in den beschriebenen Verfahren weder dezentral durch den Benutzer noch zentral durch einen Administrator noch durch die Zusammenarbeit beider zufriedenstellend erreichen.

## Zusammenfassung der Erfindung

[0013] Der Erfindung liegt das Problem zu Grunde, eine verbesserte Verarbeitungskontrolle für Objekte zu realisieren, die in ein DV-Gerät importiert oder exportiert werden sollen, oder dort verwendet werden sollen.

**[0014]** Dieses Problem wird durch ein Verfahren zur Verarbeitungskontrolle von Objekten gelöst, mit den Schritten: Erzeugen einer Kontrollanfrage durch eine Zugriffsvorrichtung bei Erfassung eines Ereignisses in Zusammenhang mit einem Objekt, wobei die Kontrollanfrage das Ereignis beschreibende Ereignisinformation und das Objekt beschreibende Objektinformation enthält;

Übertragen der Kontrollanfrage an eine Steuervorrichtung; Auswählen einer Verarbeitungsvorschrift für das Objekt aufgrund der Ereignisinformation und Objektinformation aus einem Zugriffsinformationsspeicher, der dem Objekt und dem Ereignis zugeordnete Verarbeitungsvorschriften speichert; und Verarbeiten des Objekts entsprechend der Verarbeitungsvorschrift.

**[0015]** Das Ereignis kann eine Handhabungsanweisung oder eine Anweisung für einen Übertragungsversuch über einen realen oder virtuellen Datenkanal darstellen.

**[0016]** Somit kann eine dezentrale regelbasierte Verarbeitungskontrolle für Objekte realisiert werden, die in ein DV-Gerät importiert oder exportiert werden sollen, oder dort verwendet werden sollen.

**[0017]** Weiter kann die Anweisung zur Übertragung des Objektes über den Datenkanal einen Import des Objektes in eine oder einen Export aus einer Datenverarbeitungsvorrichtung von/zu einem Peripheriegerät oder von/zu einem Netzwerk beinhalten.

**[0018]** Vorteilhaft kann eine Vielzahl von Datenkanälen kann der Zugriffsvorrichtung zugeordnet sein.

**[0019]** Zudem kann die Objektinformation Information über ein Subjekt enthalten, welches das Ereignis initiiert hat.

**[0020]** Weiter kann die Verarbeitungsvorschrift zumindest einen Schritt der folgenden Liste beinhalten:

- Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal;
- Freigabe des Imports mindestens eines Teils des Objektes und Zuordnen von lokal gültiger Zugriffsschutzinformation;
- Freigabe des Imports mindestens eines Teils des Objektes in einen gesicherten Speicherbereich;
- Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal und Auslösung von definierten Verarbeitungsschritten.

**[0021]** Das Objekt kann in Beziehung zu der Zugriffsvorrichtung und/oder dem Zugriffsinformationsspeicher stehen und die Auswahl der Verarbeitungsvorschrift kann ein Überprüfen von Attributen und/oder nachprüfbaren Qualitäten des Objektes beinhalten.

**[0022]** Die Auswahl der Verarbeitungsvorschrift kann weiter eine Berücksichtigung der Rolle des Subjektes beinhalten, welches das Ereignis initiiert hat.

**[0023]** Der Zugriffsinformationsspeicher kann einen ersten Speicherbereich mit Ereignisinformation zu einer Vielzahl von Ereignissen und einen zweiten Speicherbereich mit Objektinformation zu einer Vielzahl von Objekten enthält.

**[0024]** Weiter kann die Ereignisinformation in einer Baumstruktur mit Ereignisknoten gespeichert sein, wobei jedes Ereignis einem Ereignisknoten zugeordnet ist, und die Objektinformation in einer Baumstruktur mit Objektklassenknoten gespeichert ist, wobei jeder Objektklasse ein Objektknoten zugeordnet ist, und die Objektinformation kann eine Objektklasse und eine Objektinstanz oder eine Menge von Objektinstanzen umfassen.

**[0025]** Weiter kann vorteilhaft eine Verarbeitungsvorschrift eine Knotenverarbeitungsvorschrift oder eine Objektverarbeitungsvorschrift sein;

einem Ereignisknoten eine Objektklassenliste mit  $n \geq 0$  Objektklassen und eine Knotenverarbeitungsvorschrift zugeordnet sein, und den Objektknoten eine Knotenverarbeitungsvorschrift und Instanzlisten mit  $m \geq 0$  Listeneinträgen zugeordnet sein, wobei jeder Listeneintrag eine Instanz oder eine Instanzmenge und eine zugehörige Objektverarbeitungsvorschrift enthalten kann; und

die Objektverarbeitungsvorschrift eines Listeneintrags kann einer positiven Identifizierung zugeordnet sein, sowie die Knotenverarbeitungsvorschrift eines Ereignisknotens und die Knotenverarbeitungsvorschrift eines Objektknotens einer negativen Identifizierung.

**[0026]** Das Auswählen der Verarbeitungsvorschrift kann beinhalten:

- 15 Identifizieren des Ereignisknotens, dem der Ereignis zugeordnet ist;
- Suchen in der Objektklassenliste des identifizierten Ereignisknotens nach einer Objektklasse, die das Objekt umfasst; und
- 20 Verarbeiten des Objektes gemäß der Knotenverarbeitungsvorschrift, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, nicht enthalten ist.

**[0027]** Weiter kann die Verarbeitungsvorschrift eine positive und eine negative Teilverarbeitungsvorschrift umfassen; und

bei Erfüllung eines Ereigniskriteriums kann das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift verarbeitet werden und bei Nichterfüllung des Ereigniskriteriums das Objekt gemäß der negativen Knotenteilverarbeitungsvorschrift verarbeitet werden.

**[0028]** Das Ereigniskriterium kann mindestens ein Element der folgenden Liste betreffen:

- einen zulässigen und gültigen Objektnamen;
- einen gültigen Hashwert;
- Information über den Initiator der Objektanfrage;
- eine gültige und zulässige digitale Unterschrift;
- eine Verschlüsselung; und
- Referenzen auf notwendige Information.

**[0029]** Falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, enthalten ist kann folgendes durchgeführt werden:

- 45 Identifizieren des zugehörigen Objektklassenknotens;
- Suchen in der Instanzliste des identifizierten Objektklassenknotens nach einer Instanz, der die Instanz des Objektes entspricht;
- Auswahl der Objektverarbeitungsvorschrift, welche diesem Instanzlisteneintrag zugeordnet ist;
- 50 Verarbeitung des Objektes gemäß dieser Objektverarbeitungsvorschrift, falls eine solche gefunden wurde; und
- Verarbeitung des Objektes gemäß der Knotenverarbeitungsvorschrift des identifizierten Objektklassenknotens, falls das Objekt in der Instanzliste nicht gefunden wurde.

**[0030]** Die Knotenverarbeitungsvorschrift eines Objektknotens kann eine positive und negative Knotenteilverarbeitungsvorschrift umfassen und, falls in der Instanzliste keine dem Objekt entsprechende Instanz gefunden wurde, bei Erfüllung eines Objektknotenriteriums kann das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift verarbeitet werden und bei Nichterfüllung des Objektknotenriteriums das Objekt gemäß der negativen Knotenteilverarbeitungsvorschrift verarbeitet werden.

**[0031]** Die Objektverarbeitungsvorschriften eines Objektknotens kann positive und negative Objektteilverarbeitungsvorschriften umfassen, und wobei, falls in der Instanzliste des identifizierten Objektknotens eine dem Objekt entspre-

chende Instanz gefunden wurde und ein diesem Listeneintrag zugeordnetes Objektkriterium erfüllt ist, das Objekt gemäß der positiven Objektteilverarbeitungsvorschrift verarbeitet werden und bei Nichterfüllung des Objektkriteriums das Objekt gemäß der negativen Objektteilverarbeitungsvorschrift verarbeitet werden.

[0032] Im Falle einer Containerinstanz kann die Verarbeitungsvorschrift aus einer Anweisung bestehen, die Zugriffsentscheidung auf die Inhalte des Containers zu beziehen.

[0033] Weiter kann die Verarbeitungskontrolle verwendet werden, um Aktualisierungen in der Steuervorrichtung und/oder im Zugriffsinformationsspeicher vorzunehmen.

[0034] Ein Programm kann bereitgestellt sein, mit Instruktionen zum Ausführen der vorhergehend beschriebenen Schritte. Weiter kann ein Computer lesbares Medium bereitgestellt sein, in dem ein Programm verkörpert ist, wobei das Programm einen Computer anweist, die vorhergehend beschriebenen Schritte auszuführen. Ein Computerprogrammprodukt kann das Computer lesbare Medium umfassen.

[0035] Weiter wird das der Erfindung zugrundeliegende Problem durch eine Vorrichtung zur Verarbeitungskontrolle von Objekten gelöst, umfassend:

eine Zugriffsvorrichtung, um eine Kontrollanfrage bei Erfassung eines Ereignisses in Zusammenhang mit einem Objekt zu erzeugen, wobei die Kontrollanfrage das Ereignis beschreibende Ereignisinformation und das Objekt beschreibende Objektinformation enthält;

einen Zugriffsinformationsspeicher, um dem Objekt und dem Datenkanal zugeordnete Verarbeitungsvorschriften zu Speichern; und

eine Steuervorrichtung, um die Kontrollanfrage zu empfangen und aufgrund der Ereignisinformation und Objektinformation eine Verarbeitungsvorschrift für das Objekt auszuwählen und um eine Verarbeitung des Objekts entsprechend der Verarbeitungsvorschrift zu bewirken.

[0036] Weitere vorteilhafte Ausführungen der Erfindung sind in weiteren Ansprüchen offenbart.

#### Kurze Beschreibung der Zeichnungen

[0037] Fig. 1A zeigt in einem Flussdiagramm grundlegende Verarbeitungsschritte zur Verarbeitungskontrolle von Objekten gemäß einem Ausführungsbeispiel der Erfindung;

[0038] Fig. 1B zeigt ein Blockdiagramm des Aufbaus der Zugriffsvorrichtung zur Verarbeitungskontrolle von Objekten gemäß einem Ausführungsbeispiel der Erfindung;

[0039] Fig. 2 zeigt in einem Flussdiagramm Verarbeitungsschritte zur Verarbeitungskontrolle von Objekten gemäß einem weiteren Ausführungsbeispiel der Erfindung;

[0040] Fig. 3 zeigt in einem Flussdiagramm Verarbeitungsschritte zur Verarbeitungskontrolle von Objekten gemäß einem weiteren Ausführungsbeispiel der Erfindung;

[0041] Fig. 4 zeigt ein Blockdiagramm einer Vorrichtung zur Verarbeitungskontrolle von Objekten gemäß einem Ausführungsbeispiel der Erfindung; und

[0042] Fig. 5 veranschaulicht Knoten Der ACDB der Vorrichtung aus Fig. 4.

#### Beschreibung bevorzugter Ausführungsbeispiele

[0043] Im folgenden wird mit Bezug auf Fig. 1A ein Ausführungsbeispiel der Erfindung beschrieben.

[0044] Fig. 1A zeigt grundlegende Verarbeitungsschritte zur Verarbeitungskontrolle von Objekten, d. h. eine regelbasierte Verarbeitungskontrolle von mobiler Information auf Datenverarbeitungsvorrichtungen gemäß einem Ausführungsbeispiel der Erfindung.

[0045] Die Erfindung kann beispielsweise auf der Basis

bestehender Zugriffsschutzmechanismen in marktüblichen Betriebssystemen verwirklicht werden. Ohne den Umfang der Erfindung zu beschränken wird in Folgenden beispielhaft davon ausgegangen, dass die Zugriffsregeln von einer administrierenden Stelle gesetzt werden, die auf dem DV-Gerät des Benutzers Administrationsrechte hat. Weiter wird angenommen, dass der Benutzer des DV-Gerätes eingeschränkte Rechte hat, insbesondere um Dateien und Anwendungen auf dem DV-Gerät wirksam vor dem Zugriff des Benutzers zu schützen.

[0046] Die darauf aufbauende Verarbeitungskontrolle gemäß dem beschriebenen Ausführungsbeispiel der Erfindung führt die folgenden Schritte durch: Erzeugen einer Kontrollanfrage durch eine Zugriffsvorrichtung bei Erfassung eines Ereignisses in Zusammenhang mit einem Objekt in einem Schritt 101, wobei die Kontrollanfrage das Ereignis beschreibende Ereignisinformation und das Objekt beschreibende Objektinformation enthält; Übertragen der Kontrollanfrage an eine Steuervorrichtung in einem Schritt 102; Auswählen einer Verarbeitungsvorschrift für das Objekt aufgrund der Ereignisinformation und Objektinformation aus einem Zugriffsinformationsspeicher, der dem Objekt und dem Ereignis zugeordnete Verarbeitungsvorschriften speichert in einem Schritt 103; und Verarbeiten des Objekts entsprechend der Verarbeitungsvorschrift in einem Schritt 104.

[0047] Dabei kann die Entscheidung über das Verfahren mit dem Objekt unter Berücksichtigung des Weges getroffen werden, auf dem das Objekt zu oder aus einem DV-Gerät gelangt, und/oder unter Berücksichtigung von Attributen und Qualitäten des Objektes und/oder unter Berücksichtigung einer Rolle, die dem Subjekt zugeordnet ist, welches das Verfahren initiiert hat. Das Ergebnis der Entscheidung ist vorzugsweise das Setzen von Zugriffsschutzinformation für das kontrollierte Objekt sowie die Durchführung einer definierten Menge von Verarbeitungsschritten.

[0048] Die Entscheidung über die Verarbeitung des Objekts kann insbesondere von folgenden Faktoren abhängig gemacht werden:

- Attribute oder nachprüfbare Qualitäten des Objektes, wie z. B. die Integrität.
- Freigabe oder Sperrung des Objektes durch eine dazu berechnete Instanz.
- Kommunikationsweg über den das Objekt transportiert werden soll.
- Zugehörigkeit zu einer oder mehreren Objektklassen.

[0049] Das Ergebnis der Überprüfung kann dabei nicht nur die digitale Entscheidung ja/nein sein, sondern kann ein Verfahren definieren, wie mit dem Objekt vorgegangen wird. Beim Import bzw. Export von Daten können solche Verfahren beispielsweise sein:

- Ablehnung des Imports bzw. Exports des Objektes oder eines Teils des Objektes.
- Import des Objektes, Anfügen von lokal gültiger Zugriffsschutzinformation entsprechend der Sicherheitspolitik, welche die Verwendungsmöglichkeit durch den Anwender festlegt
- Import des Objektes auf das System in einen Speicherbereich, der nicht zum Zugriff durch das Subjekt freigegeben ist. Gegebenenfalls Gewährung des Zugriffs durch definierte Applikationen.
- Auslösung von definierten Verarbeitungsschritten beim Transport oder Transportversuch eines Objektes; z. B. erzeugen eines Log-Eintrags oder kontrollierte In-

stallation einer Software ohne Benutzerinteraktion.

[0050] Bei der lokalen Verwendung von Objekten können solche Verfahren sein:

- Durchführung oder Ablehnung der angeforderten Verfahrensweise und gegebenenfalls Auslösung weiterer Verarbeitungsschritte, wie zum Beispiel Erzeugen eines Log-Files.
- Ersetzen der angeforderten Verfahrensweise durch eine andere Verfahrensweise, die durch das Verarbeitungskontrollsystem definiert wird.

[0051] Es ist möglich, dass das zu erfassende Ereignis dabei eine Handhabungsanweisung oder einen Übertragungsversuch nicht nur über einen realen, sondern auch über einen virtuellen Datenkanal darstellt.

[0052] Im folgenden wird mit Bezug auf Fig. 1B ein weiteres Ausführungsbeispiel der Erfindung beschrieben.

[0053] Fig. 1B zeigt den Aufbau der Zugriffsvorrichtung zur Verarbeitungskontrolle von Objekten gemäß einem Ausführungsbeispiel der Erfindung.

[0054] Die Ereignisse, allgemein mit 1.1 bezeichnet werden durch Softwarekomponenten 1.2 im DV-Gerät identifiziert, wie z. B. Gerätetreiber, Dienste oder Betriebssystemkomponenten, die unter dem Schutz der lokalen Systemrechte stehen und auf die von einem Benutzbereich 1.6 nicht zugegriffen werden kann. Diese Softwarekomponenten werden ergänzt durch neue Software-Komponenten, welche die Ereignisse registrieren und die Verarbeitungskontrolle initiieren.

[0055] Diese neuen Software-Komponenten werden Event-Proxies (EP) 1.3 genannt. Im Fall einer Handhabungsanweisung wird diese vor der Übergabe an das Betriebssystem von der neuen Komponente entgegengenommen und bearbeitet, im Fall eines Datentransports wird dieser durch die neue Komponente kontrolliert.

[0056] Der Zugriffsinformationsspeicher 1.4 wird auf dem DV-Gerät unter Administratorrechten gehalten und implementiert die Zugriffsschutzpolitik. Dieser Speicher heißt Access Control Data Base (ACDB).

[0057] Das Ergebnis der Kontrollanfrage ist eine Verarbeitungsvorschrift 1.5.

[0058] Im folgenden wird ein Beispiel für die Funktionalität eines Event Proxies beschrieben

[0059] Registriert ein Event Proxy ein Ereignis, so liefert ihm die ACDB die notwendigen Informationen zur Durchführung des Kontrollprozesses für das betroffene Objekt. Beim Wunsch des Datenimports muss hierzu möglicherweise ein Teil oder alle Daten in das DV-Gerät übertragen werden, jedoch in einen Speicherbereich, der vor dem Benutzer geschützt ist.

[0060] Das Ergebnis des Kontrollprozesses kann die Durchführung einer in der ACDB definierten Verarbeitungsvorschrift durch das EP sein, welche zumindest einen Schritt der folgenden Liste beinhaltet:

- Sperrung der Übertragung des Objekts und Löschen der zur Entscheidungsfindung bereits auf den Rechner gelangten Daten;
- Freigabe der Übertragung des Objekts über einen Datenkanal;
- Freigabe des Imports mindestens eines Teils des Objekts und
- Zuordnen lokal gültiger Zugriffsschutzinformation;
- Freigabe des Imports mindestens eines Teils des Objekts in einen gesicherten Speicherbereich;
- Freigabe oder Sperrung der Übertragung des Objekts

über einen Datenkanal und Auslösen von definierten Aktionen bzw. Verarbeitungsschritten. Aktionen können dabei objektunabhängig sein z. B. Erzeugen eines Logs, ein Verarbeitungsschritt kann sich auf das Objekt beziehen.

[0061] Im folgenden wird ein Beispiel für den Aufbau der Access Control Data Base beschrieben.

[0062] Dabei kann der Zugriffsinformationsspeicher, die ACDB, einen ersten Speicherbereich enthalten, mit Ereignisinformation zu einer Vielzahl von Ereignissen und einen zweiten Speicherbereich mit Objektinformation zu einer Vielzahl von Objekten.

[0063] Weiter kann die Ereignisinformation in einer Baumstruktur mit Ereignisknoten gespeichert sein, wobei jedes Ereignis einem Ereignisknoten zugeordnet ist, und die Objektinformation kann in einer Baumstruktur mit Objektklassenknoten gespeichert sein, wobei jeder Objektklasse ein Objektklassenknoten zugeordnet ist.

[0064] In beiden Bäumen der ACDB sind jeweils Knoten Generalisierungen darunter liegender Knoten.

[0065] Das im Folgenden beschriebene Beispiel für ein Regelwerk zur Abarbeitung dieser Bäume bestimmt das Ergebnis einer Kontrollanfrage eines EP. Dieses Ergebnis besteht aus einer Verarbeitungsvorschrift.

[0066] Der erste Baum beschreibt die Ereignisse (Event Tree, ET). Die Wurzel des ET steht für "alle Ereignisse". Jedem Event-Proxy des DV-Gerätes ist eindeutig ein Knoten des ET zugeordnet. Der ET kann weitere Knoten enthalten, die nicht eindeutig Event-Proxies zugeordnet sind. Diese Knoten heißen Ereignisknoten.

[0067] Der zweite Baum beschreibt die Objektklassen (Object Tree, OT). Die Wurzel des OT steht für "alle Objektklassen", die Knoten entsprechen Objektklassen und heißen Objektklassenknoten.

[0068] Im folgenden wird ein Beispiel für die Attribute der Ereignisknoten und der Objektklassenknoten beschrieben. Knoten und Blätter beider Bäume haben Attribute. Diese können mit Vererbungsregeln versehen werden.

[0069] Das Attribut V (Verarbeitungsvorschrift) tritt in beiden Bäumen auf und enthält Verarbeitungskontrollinformation. Attribut V setzt sich zusammen aus den Teilattributen K (Kriterium), V1 (positive Teilverarbeitungsvorschrift) und V2 (negative Teilverarbeitungsvorschrift). Das Teilattribut Kriterium enthält ein Entscheidungsverfahren mit den möglichen Ergebnissen ja oder nein, sowie alle Informationen oder Referenzen auf Informationen, die zur Abwicklung des Entscheidungsverfahrens notwendig sind. Dies können z. B. Listen von Zertifikaten sein, Listen von Instanzen mit zugehörigen Berechtigungen, Hashwerte und anderes.

[0070] Das Kriterium betrifft mindestens ein Element der folgenden Liste:

- einen zulässigen und gültigen Objektnamen
- einen gültigen Hashwert
- Information über den Initiator des Ereignisses
- eine gültige und zulässige digitale Unterschrift
- eine Verschlüsselung und
- Referenzen auf notwendige Informationen

[0071] Das Teilattribut "positive Teilverarbeitungsvorschrift" definiert die durchzuführenden Verarbeitungsschritte bei Ergebnis "ja", und das Teilattribut "negative Teilverarbeitungsvorschrift" definiert durchzuführende Verarbeitungsschritte bei Entscheidung "nein".

[0072] ET und OT Knoten besitzen jeweils 2 Attribute, eine Knotenverarbeitungsvorschrift und eine Liste:

Das erste Attribut jedes ET-Knotens ist Attribut V, die Kno-

tenverarbeitungsvorschrift, welche direkt oder durch Vererbung mit Werten belegt sein muss.

[0073] Das zweite Attribut der Ereignisknoten ist Attribut OL (Objektklassenliste). Es besteht aus einer Liste vom Typ Attribut O (Objektklasse), das als Wert einen Knotennamen des OT enthält. Jeder OT-Knotenname darf nur einmal in der Liste auftauchen. Die Liste OL kann auch leer sein.

[0074] Das erste Attribut jedes Objektklassenknoten ist wieder Attribut V, eine Knotenverarbeitungsvorschrift, welche direkt oder durch Vererbung mit Werten belegt sein muss.

[0075] Das zweite Attribut der Objektklassenknoten ist Attribut IL (Instanzenliste). Jedes Listenelement setzt sich zusammen aus den Teilattributen Attribut I (Instanzenmenge) und Attribut V, der Objektverarbeitungsvorschrift. Der Wert von Attribut I identifiziert eine Instanz oder eine Menge von Instanzen der zugehörigen Objektklasse. Die Liste kann auch leer sein.

[0076] An den einzelnen Knoten können auch noch Policy Parameter definiert sein, welche die Abarbeitung der Listen steuern, z. B. first hit, first positive hit, first negative hit. Ohne Einschränkung der Allgemeinheit wird im Folgenden der Fall einer sequentiellen Abarbeitung der Attributlisten mit der Regel "first hit" beschrieben.

[0077] Im Überblick weist das oben beschriebene Beispiel folgendes auf:

#### Ereignisknoten

1. Attribut V (Knotenverarbeitungsvorschrift)
  2. Attribut OL (Objektklassenliste)
- Liste von Attribut O (Objektklasse)

#### Objektklassenknoten

1. Attribut V (Knotenverarbeitungsvorschrift)
  2. Attribut IL (Instanzenliste)
- Liste von  
Attribut I (Instanzenmenge)  
Attribut V (Objektverarbeitungsvorschrift)

[0078] Im folgenden wird mit Bezug auf Fig. 2 und 3 ein weiteres Ausführungsbeispiel der Erfindung beschrieben. Fig. 2 und 3 zeigen beispielhaft Aktivitätsdiagramme des Ablaufs einer Zugriffsentscheidung.

[0079] Bei Registrierung eines Ereignisses durch einen Proxy in einem Schritt 2.1 wird zunächst das zugehörige Objekt identifiziert sowie versucht das Subjekt zu identifizieren, welches das Ereignis ausgelöst hat.

[0080] Somit kann die Objektinformation Informationen über ein Subjekt enthalten, welches die Kontrollanfrage initiiert hat.

[0081] Anschließend wird der eindeutig dem Proxy zugeordnete Ereignisknoten in Schritt 2.2 besucht. Ist die Objektklassenliste dieses Knotens leer, so wird in Schritt 2.3 und 2.6 entsprechend der Knotenverarbeitungsvorschrift in Attribut V weiterverfahren. Dies kann z. B. der Fall sein, wenn der Datenverkehr über einen Kanal für alle Daten gleichen Restriktionen unterworfen ist, z. B. vollständig gesperrt, Eintrag in Logfile bei Zugriffsversuch.

[0082] Sind Einträge in der Objektklassenliste vorhanden, so versucht in Schritt 2.3 das Proxy der identifizierten Objektinstanz eine Objektklasse aus dieser Liste zuzuordnen. Dabei wird die Liste sequentiell abgearbeitet. Gelingt die Zuordnung nicht, so wird in Schritt 2.6 wieder vorgegangen wie in der Knotenverarbeitungsvorschrift vorgesehen.

[0083] Bei der ersten identifizierten Objektklasse wird in Schritt 2.4 der entsprechende Objektklassenknoten des OT

untersucht. Auch hier wird die Instanzenliste sequentiell abgearbeitet und gesucht, ob die konkrete Instanz an Hand des Attributs I identifiziert werden kann. Wird dabei kein passender Eintrag gefunden, wird in Schritt 2.7 entsprechend dem Knotenverarbeitungsvorschrift vorgegangen. Sobald die erste passende Instanz gefunden ist, wird in Schritt 2.5 nach der zugehörigen Objektverarbeitungsvorschrift verfahren.

[0084] In jedem Fall ist in diesem Beispiel also dem identifizierten Objekt jetzt eine Verarbeitungsvorschrift zugeordnet worden.

[0085] In Schritt 3.1 wird das Kriterium der Vorschrift überprüft. Kriterium könnte dabei z. B. sein, dass der Benutzer ein Administrator ist, oder dass eine gültige digitale Unterschrift eines berechtigten zu der Instanz vorhanden ist. Bei Bedarf werden in Schritt 3.5 weitere Informationen beschafft, die zur Entscheidungsfindung notwendig sind, z. B. Zertifikate oder Hashwerte. Wird in Schritt 3.2 die Entscheidung "ja" getroffen, so werden in Schritt 3.3 die in der positiven Teilverarbeitungsvorschrift definierten Aktionen durchgeführt. Wird die Entscheidung "nein" getroffen, oder kann die zur Entscheidungsfindung notwendige Information nicht vollständig beschafft werden, so werden in Schritt 3.6 die in der negativen Teilverarbeitungsvorschrift definierten Aktionen durchgeführt. Sowohl positive als auch negative Teilverarbeitungsvorschrift definieren Verarbeitungsschritte, die nun in Schritt 3.7 ausgeführt werden können.

[0086] Im Falle einer Containerinstanz kann die Vorschrift auch aus der Anweisung bestehen, die Zugriffsentscheidung auf die Inhalte des Containers zu beziehen. In diesem Fall wird für jedes Objekt des Containers das gleiche Ereignis ausgelöst wie für den Container selbst und beginnend mit Schritt 2.1 mit den Objekten des Containers analog verfahren.

[0087] Für die Inhalte der Teilverarbeitungsvorschriften sind keine Einschränkungen vorhanden. So kann im positiven Fall die Verarbeitung z.B. darin bestehen, dass ein Programm importiert wird und sich selbst (ohne Benutzereinwirkung) in einer festgelegten Konfiguration und mit definierten Zugriffsrechten auf dem Rechner installiert. In jedem Fall können beispielsweise auch Audit Records geschrieben werden oder weitere Aktionen ausgelöst werden.

[0088] In der beschriebenen Ausführung kann die Objektinformation eine Objektklasse und eine Objektinstanz oder eine Menge von Objektinstanzen umfassen.

[0089] Weiter kann in dieser Ausführung eine Verarbeitungsvorschrift eine Knotenverarbeitungsvorschrift oder eine Objektverarbeitungsvorschrift sein; Weiter kann einem Ereignisknoten ist eine Knotenverarbeitungsvorschrift und eine Objektklassenliste mit  $n \geq 0$  Objektklassen zugeordnet sein, und den Objektklassenknoten eine Knotenverarbeitungsvorschrift und eine Instanzliste mit  $m \geq 0$  Listeneinträgen, wobei jeder Listeneintrag eine Instanz oder eine Instanzmenge und eine zugehörige Objektverarbeitungsvorschrift enthält; und die Objektverarbeitungsvorschrift eines Listeneintrags kann einer positiven Identifizierung zugeordnet sein, sowie die Knotenverarbeitungsvorschrift eines Ereignisknotens und die Knotenverarbeitungsvorschrift eines Objektklassenknotens einer negativen Identifizierung.

[0090] Das Auswählen der Verarbeitungsvorschrift kann beinhalten: Identifizieren des Ereignisknotens, dem das Ereignis zugeordnet ist; Suchen in der Objektklassenliste des identifizierten Ereignisknotens nach einer Objektklasse, die das Objekt umfasst; und Verarbeiten des Objekts gemäß der Knotenverarbeitungsvorschrift, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, nicht enthalten ist.

[0091] Falls in der Objektklassenliste des identifizierten

Ereignisknotens eine Objektklasse, die das Objekt umfasst, enthalten ist: Identifizieren des zugehörigen Objektklassenknotens; Suchen in der Instanzliste des identifizierten Objektklassenknotens nach einer Instanz der die Instanz des Objektes entspricht; Auswahl der Objektverarbeitungsvorschrift, welche diesem Instanzlisteneintrag zugeordnet ist; Verarbeitung des Objektes gemäß dieser Objektverarbeitungsvorschrift, falls eine solche gefunden wurde; und Verarbeitung des Objektes gemäß der Knotenverarbeitungsvorschrift des identifizierten Objektklassenknotens, falls das Objekt in der Instanzliste nicht gefunden wurde.

[0092] Bei diesem Beispiel kann die Knotenverarbeitungsvorschrift der Ereignisknoten eine positive und eine negative Knotenteilverarbeitungsvorschrift umfassen; und bei Erfüllung eines Ereigniskriteriums wird das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift und bei Nichterfüllung des Ereigniskriteriums gemäß der negativen Knotenteilverarbeitungsvorschrift verarbeitet.

[0093] Somit kann die oben beschriebene Verarbeitungskontrolle verwendet werden, um Aktualisierungen in der Steuervorrichtung und/oder im Zugriffsinformationsspeicher vorzunehmen.

[0094] Weiter kann die Knotenverarbeitungsvorschrift eines Objektklassenknotens eine positive und eine negative Knotenteilverarbeitungsvorschrift umfassen, und falls in der Instanzliste keine dem Objekt entsprechende Instanz gefunden wurde, wird bei Erfüllung eines Objektklassenknotenskriteriums das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift verarbeitet und bei Nichterfüllung des Ereigniskriteriums gemäß der negativen Knotenteilverarbeitungsvorschrift.

[0095] Ebenso kann im dargestellten Verfahren die Objektverarbeitungsvorschriften eines Objektklassenknotens positive und negative Objektteilverarbeitungsvorschriften umfassen, wobei, falls in der Instanzliste des identifizierten Objektklassenknotens eine dem Objekt entsprechende Instanz gefunden wurde und ein diesem Listeneintrag zugeordnetes Objektkriterium erfüllt ist, das Objekt gemäß der positiven Objektteilverarbeitungsvorschrift verarbeitet wird und bei Nichterfüllung des Objektkriterium gemäß der negativen Objektteilverarbeitungsvorschrift verarbeitet wird.

[0096] Im folgenden wird ein Beispiel einer Administration des Zugriffsschutzsystems beschrieben

#### Erstinstallation

[0097] Die ACDB wird angelegt. Dabei werden von ET und OT jeweils die Wurzeln installiert und deren Attribute gesetzt. Das Attribut 1 bleibt jeweils leer; der Wert der Attribute 2 wird durch die Security Policy bestimmt. Bei einer Vererbung der Attribute auf die Nachkommen bedeutet beispielsweise ein "Vollzugriff für Administration" als Attribut 2 im den Wurzeln von ET und OT, dass die Administration alle installierten Kanäle ohne Einschränkungen verwenden kann. Für den normalen Benutzer hat dieses Attribut die Regel "alles was nicht erlaubt ist, ist verboten" zur Folge.

[0098] Ein Default Proxy wird installiert und allen vorhandenen Datenkanälen zugeordnet. Diesem Proxy wird die Wurzel des ET als Knoten zugeordnet, es kann die dort enthaltenen Attribute verarbeiten.

[0099] Das Betriebssystem wird so angepasst, dass jede Installation eines neuen realen Datenkanals automatisch die Einbindung eines EP mit Zuordnung eines Knotens des ET nach sich zieht. Wird dieses EP nicht durch die Administration explizit installiert, so wird standardmäßig das Default Proxy installiert.

[0100] Für die Administration wird eine Schnittstelle zur Bearbeitung der ACDB bereitgestellt. Installation von wei-

teren (von realen Datenkanälen unabhängigen) Ereignistypen mit ihren Proxies wie auch die Administration der ACDB kann sowohl interaktiv durch einen Administrator als auch durch ein Programm, das unter Administratorrechten abläuft, durchgeführt werden.

#### Administration

[0101] In den ET und den OT können Knoten gelöscht werden, Attribute geändert werden und neue Knoten hinzugefügt und mit Attributen versehen werden.

[0102] Beim Hinzufügen eines neuen Ereignistyps wird die Einrichtung eines EPs angefordert. Wird dieses explizit installiert, so muss ihm ein Knoten des ET zugeordnet werden. Geschieht diese Zuordnung nicht, wird die Wurzel zugeordnet. Soll ein neuer Knoten erzeugt und zugeordnet werden, so erfolgt dies wie oben beschrieben. Die Entfernung eines Ereignisses hat nicht automatisch die Entfernung des EP und des entsprechenden Knoten zur Folge; das EP kann von mehreren Kanälen genutzt werden, ein Knoten kann zu mehreren EPs gehören, ein Knoten kann auch ohne Zuordnung zu EPs im Baum existieren.

#### Update Mechanismen – Kontrollklassen

[0103] Ein Update des Verarbeitungskontrollsystems muss nicht durch einen Administrator vor Ort vorgenommen werden, das bereits installierte Kontrollsystem kann im Bootstrapping Verfahren verwendet werden, indem etwa ein Updateprogramm durch eine berechtigte Unterschrift als importierbar und ausführbar gekennzeichnet wird. Ein solches Update kann z. B. bei jeder Netzanmeldung des Benutzers automatisch vorgenommen werden (ohne Beteiligung des Benutzers), dies ist das online-Modell der Administration, oder durch den Benutzer mit Hilfe einer CD oder Diskette (offline Modell).

[0104] Die Entscheidungskriterien zur Verarbeitungskontrolle für konkrete Objekte können von der Administration in verschiedenen Sicherheitsleveln festgelegt werden. Einige mögliche Level sind die folgenden:

low 1: die Entscheidung basiert auf einem ungesichertem Teil der zu importierenden Daten, wie z. B. dem Namen eines Containers.

low 2: die Entscheidung basiert auf dem ungesicherten Hashwert des vollständigen zu importierenden Datums.

medium: die Entscheidung basiert auf einer digitalen Unterschrift unter das zu importierende Datum.

high: die Entscheidung basiert auf einer digitalen Unterschrift unter das verschlüsselte zu importierende Datum, wobei der Schlüssel ein Eintrag am entsprechenden Attribut der ACDB ist.

[0105] In den folgenden Beispiele wird die Erfindung anhand weiterer konkreter Ausprägungen erläutert:

In einem ersten Beispiel wird ein virtueller Datenkanal betrachtet

[0106] Der Kassenbestand einer Bank soll revisionssicher verwaltet werden. Es wird davon ausgegangen, dass sich der Geldbestand nur bei geöffneter Kasse ändern kann. Bei geöffneter Kasse soll stets eine Videoüberwachung gestartet werden. Diese Überwachung hält an bis die Kasse wieder geschlossen wird. Stimmt beim Tagesabschluss die Kasse nicht, können alle Vorgänge mit der Aufzeichnung abgeglichen werden.

[0107] Der einzige Datenkanal in diesem System ist der Geldtransport von und zur Kasse. Das Ereignis, dass vom einzigen Proxy des EDV-Systems der Bank registriert wird, ist der Wunsch zum Öffnen der Kasse (siehe 2.1). Der zugehörige Ereignisbaum besteht aus einem einzigen Ereignis-

knoten mit leerer Objektklassenliste und der Knotenverarbeitungsvorschrift (siehe 2.6) "Kasse öffnen und Videoüberwachung einschalten bis Kasse wieder geschlossen", die in jedem Fall durchgeführt wird.

[0108] In einem zweiten Beispiel wird ein datenkanalunabhängiges Ereignis betrachtet.

[0109] In einer Umgebung mit der Notwendigkeit des Archivierens juristisch relevanter Tatbestände ist in einem Betriebssystem trotzdem der Standardbefehl "Datei löschen" bekannt. Führt ein Benutzer diesen Befehl mit Daten durch, die archiviert werden müssen, so wird dieser Befehl durch die Erfindung so modifiziert, dass die Anfrage "Datei löschen" durch ein Kopieren auf den Archivbestand ersetzt wird, und erst nach positiver Rückmeldung des Kopierens der lokale Datenbestand gelöscht wird. Entsprechend können andere Betriebssystembefehle modifiziert werden.

[0110] Der einzige Proxy des Systems fängt die Befehle der Shell ab und untersucht sie. Das ausgelöste Ereignis (siehe 2.1) lautet "Betriebssystembefehl empfangen". Das in (siehe 2.2) identifizierte Objekt besteht aus dem vollständigen Befehl einschließlich aller Parameter. Das Subjekt ist der Eigentümer der Shell. Es gibt nur einen Ereignisknoten. Dieser enthält eine Liste von Objektklassen die durchsucht wird (siehe 2.3). Diese sind Betriebssystembefehle mit Parameterklassen:

Ereignisknoten "Betriebssystembefehl":

Knotenverarbeitungsvorschrift:

"führe Befehl entsprechend den Rechten des Subjekts aus."

Objektklassenliste:

O1: "rm im Verzeichnis /xyz"

O2: "mv mit Quelle im Verzeichnis /xyz"

O3: "mv mit Ziel im Verzeichnis /xyz"

OX: "sonstige Befehle im Verzeichnis /xyz"

[0111] In den zugehörigen Objektklassenknoten werden die Verarbeitungsvorschriften definiert. Dabei kann in der Instanzenliste dieser Knoten z. B. für Unterverzeichnisse von /xyz noch unterschiedliches Vorgehen angefordert werden. Trifft ein rm-Befehl ein, so wird auf den zugehörigen Objektklassenknoten verzweigt (2.4). Der Objektklassenknoten zu "rm im Verzeichnis /xyz" könnte wie folgt aussehen:

Objektklassenknoten "rm im Verzeichnis /xyz":

Knotenverarbeitungsvorschrift:

Kriterium: Benutzer darf auf /xyz schreiben

Pos. Teilverarbeitungsvorschrift: "Kopiere auf Archivbestand /xyz/abc, führe anschließend Befehl durch"

Neg. Teilverarbeitungsvorschrift: "Befehl ablehnen"

Instanzenliste:

I1: "rm im Verzeichnis /xyz/abc"

V1: "Befehl immer ablehnen"

[0112] Besitzt das Subjekt Schreibberechtigung auf /xyz, so kann er eine Datei löschen, diese wird allerdings dann in ein Verzeichnis kopiert (z. B. auf ein Magnetband), für welches kein Subjekt Löschberechtigung hat.

[0113] Fig. 4 zeigt ein Blockdiagramm einer Vorrichtung zur Verarbeitungskontrolle von Objekten gemäß einem Ausführungsbeispiel der Erfindung. In einem dritten Beispiel wird nunmehr unter Bezug auf Fig. 4 ein Notebook mit realen Datenkanälen betrachtet.

[0114] In dem im Folgenden beschriebenen Ausführungsbeispiel (vergleiche Fig. 4) beinhaltet die Übertragung des Objektes über den Datenkanal einen Import in eine oder einen Export aus einer Datenverarbeitungsvorrichtung von/zu einem Peripheriegerät oder von/zu einem Netzwerk.

[0115] Weiter kann in diesem Beispiel der Zugriffsvorrichtung eine Vielzahl von Datenkanälen zugeordnet sein.

[0116] Die Datenverarbeitungsvorrichtung ist ein Notebook, das in ein Netzwerk eingebunden ist, aber nicht immer

online sein muss. Dabei wird die folgende Konfiguration gewünscht: Drucken ist dem Benutzer über die lokal installierten Drucker ljl 4.1 und lj2 4.2 ohne Einschränkungen erlaubt. Diese Drucker werden durch die entsprechenden Treiber 4.6 und 4.7 angesteuert. Für alle Drucker ist nur ein Drucker-Proxy 4.12 installiert. Als Datenkanal ist für einen bestimmten Benutzer CD 4.3 mit dem zugehörigen Treiber 4.8 und Proxy 4.13 zugelassen. Über das CD-Laufwerk ist das Lesen von CDs möglich, die von der Administration freigegeben sind. Ausführbare Dateien sind jedoch vom Anwender nicht über CD-Laufwerk importierbar. Audio und Video-Daten können über CD generell gelesen werden; Videos jedoch nur über einen definierten Player.

[0117] Als Netzdienste sind ftp 4.9 zum Import bestimmter zip-Dateien sowie http 4.10 über den Intranet-Proxy erlaubt. Diese werden über die Netzkarte 4.4 abgewickelt. Für diese beiden Dienste müssen Proxies 4.14, 4.15 installiert werden.

[0118] Das Update des Notebooks soll sowohl über CD als auch über ftp möglich sein.

[0119] Andere Datenkanäle 4.5 mit ihren zugehörigen Treibern 4.11, z. B. Diskette, Modem sind gesperrt und nur durch bestimmte Administratoren verwendbar. Für alle diese weiteren Kanäle ist das Default Proxy 4.17 zuständig.

[0120] Die Verarbeitungsvorschrift wird durch ein Proxy unter Verwendung der ACDB 4.14 ausgewählt.

[0121] Die ausgewählte Verarbeitungsvorschrift kann erlauben, dass der Benutzer die Daten in seinen Bereich 4.18 importiert oder dass er mit eigenen Applikationen 4.19 auf Daten zugreift.

[0122] Es ist aber auch möglich, dass Daten zunächst in den Sicherheitsbereich 4.20 importiert werden, auf den der Benutzer keinen Zugriff hat. Die Verarbeitungsvorschrift kann dann nach Abschluss des Kontrollvorgangs diese Daten entweder wieder löschen, oder dem Benutzer zur Verwendung zur Verfügung stellen, oder den Zugriff durch Sicherheitsapplikationen 4.21 erlauben oder steuern.

[0123] Im folgenden wird mit Bezug auf Fig. 5 ein weiteres Ausführungsbeispiel der Erfindung beschrieben.

[0124] Fig. 5 stellt den Aufbau der beiden Bäume der ACDB des Beispiels von Fig. 4 dar. Dabei wird bei der Abarbeitung der Listen vom Prinzip "first hit" ausgegangen. Im Folgenden werden die Attribute der beiden Bäume zusammengestellt.

Attribute im Event Tree

alle Ereignisse 5.1

50 Knotenverarbeitungsvorschrift:

K: Benutzer ist Administrator xy?

pV: Vollzugriff erlaubt, erzeuge Log.

nV: Kein Zugriff, lösche bereits importierte Daten, schreibe Log.

55 Objektklassenliste: leer

Drucker 5.2

Knotenverarbeitungsvorschrift:

K: immer ja

pV: drucken erlaubt.

nV: -

Objektklassenliste: leer

CD 5.3

Knotenverarbeitungsvorschrift:

Geerbt von "alle Ereignisse"

## Objektklassenliste:

O1: Container CD-Inhalt  
 O2: Container Dateiverzeichnis  
 O3: Ausführbare Dateien (\*.exe, \*.bat, \*.com, \*.dll)  
 O4: Audio  
 O5: Video  
 O6: ZIP

## Netzdienste 5.4

## Knotenverarbeitungsvorschrift:

Geerbt von "alle Ereignisse"

## Objektklassenliste:

O1: leer

## ftp 5.5

## Knotenverarbeitungsvorschrift:

K: immer nein

pV: -

nV: Warnung an Benutzer, lösche bereits importierte Daten.

## Objektklassenliste:

O1: ZIP

## http 5.6

## Knotenverarbeitungsvorschrift:

K: Partner = Intranet Proxy?

pV: lesen und schreiben erlaubt.

nV: Warnung an Benutzer

## Objektklassenliste: leer

## Attribute im Object Tree

## alle Objektklassen 5.7

## Knotenverarbeitungsvorschrift:

K: Benutzer ist Administrator xy?

pV: Vollzugriff erlaubt, erzeuge Log

nV: Kein Zugriff, lösche bereits importierte Daten, schreibe Log.

## Instanzenliste: leer

## CD-Inhalt 5.8

## Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen"

## Instanzenliste:

I1: alle mit Unterschrift

V1: K: Unterschrift von uvw enthalten?

pV: importiere setup.exe in Sicherheitsbasis, führe setup aus, erlaube setup Zugriff auf CD, schreibe Log

nV: falls ungültige Unterschrift: schreibe Log, warne Benutzer. Falls ohne Unterschrift: überprüfe Inhalt des Containers  
 I2: alle

V2: K: CD-ID lokal vorhanden und Hashwert stimmt mit lokalem Hashwert überein?

pV: gebe CD-Inhalt zum Import frei

nV: überprüfe Inhalt des Containers

## Dateien 5.9

## Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen"

## Instanzenliste: leer

## Dateiverzeichnis 5.10

## Knotenverarbeitungsvorschrift:

K: immer ja

5 pV: überprüfe Inhalt des Verzeichnisses

nV: -

## Instanzenliste: leer

## ausführbare Dateien 5.11

10

## Instanzenliste: leer

## Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen"

15

## ZIP 5.12

## Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen"

## Instanzenliste:

20 I1: name = "acupdate.zip"

V1: K: Anfrage kommt von OT Knoten "ftp" oder "CD" und Unterschrift von Berechtigtem enthalten?

pV: importiere in Sicherheitsbasis, entpacke, führe setup aus, falls noch nicht geschehen, schreibe Log

25 nV: warne Benutzer, schreibe Log

I2: name = "angebotsdaten.zip"

V2: K: Anfrage kommt von OT Knoten "ftp" und Unterschrift von Berechtigtem enthalten?

pV: importiere in Sicherheitsbasis, entpacke, kopiere Inhalt in Angebotsverzeichnis, schreibe Log

30 nV: warne Benutzer, schreibe Log

## Multimedia 5.13

## 35 Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen"

## Instanzenliste: leer

## Audio 5.14

## Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen" Instanzenliste:

I1: alle

V1: K: immer ja

45 pV: Zugriff durch beliebige Benutzerapplikation erlaubt

nV: -

## Video 5.15

## 50 Knotenverarbeitungsvorschrift:

geerbt von "alle Objektklassen" Instanzenliste:

I1: alle

V1: K: immer ja

pV: Zugriff durch definierte Applikation erlaubt

55 nV: -

[0125] Für die folgenden Fälle soll der Ablauf der Verarbeitungskontrolle in diesem konkreten Beispiel beschrieben werden:

## 60 Lesen von Dateien von einer nicht freigegebenen CD

[0126] In diesem Beispiel steht das Objekt in Beziehung zu der Zugriffsvorrichtung und/oder dem Zugriffsinformationsspeicher. Dabei beinhaltet die Auswahl der Verarbeitungsvorschrift ein Überprüfen von Attributen und/oder nachprüfaren Qualitäten des Objekts.

[0127] Ebenso beinhaltet die Auswahl der Verarbeitungsvorschrift eine Berücksichtigung der Rolle des Subjekts.

welches die Kontrollanfrage initiiert hat.

[0128] Der CD-Proxy 4.14 erkennt, dass eine CD eingelegt wird (siehe 2.1). Im CD-Ereignisknoten 5.3 wird als Objekt ein CD-Inhalt ohne Signatur identifiziert (siehe 2.2). Der passende Listeneintrag (siehe 2.3) hierzu ist die Objektklasse CD-Inhalt. Der entsprechenden Knoten 5.8 im OT wird besucht. Dort wird die Liste der Instanzen abgearbeitet (siehe 2.4) und die Objektverarbeitungsvorschrift der zweiten Instanzenmenge ("alle") ausgeführt (siehe 2.5). Ist die CD-ID in einer lokalen Datenbasis bekannt, so wird der Hashwert der CD gebildet und mit dem lokal vorhandenen Hashwert verglichen (siehe 3.5). Stimmen diese überein, so ist die CD freigegeben und das Objektklassenkriterium ergibt "ja" (siehe 3.2). Die positive Teilverarbeitungsvorschrift wird durchgeführt (siehe 3.3), die CD kann vom Benutzer frei verwendet werden. Ist die CD-ID nicht bekannt, so gibt es auch keinen Hashwert in der lokalen Datenbasis, das Kriterium ergibt "nein", genau wie im Fall eines ungültigen Hashwertes und die negative Teilverarbeitungsvorschrift wird durchgeführt (siehe 3.6). Der Proxy importiert daraufhin das Dateiverzeichnis und überprüft die Objektklassen der einzelnen Dateien. Im CD-Ereignisknoten 5.3 können Dateiverzeichnisse, Audio, Video, Zip und ausführbare Dateien identifiziert werden und dann der entsprechende Objektklassenknoten besucht werden.

[0129] Bei Verzeichnissen 5.10 wird wieder der Inhalt überprüft, bis schließlich auf Dateien gestoßen wird.

[0130] Bei ausführbaren Dateien 5.11 ergibt das Kriterium im zugehörigen Objektklassenknoten für einen gewöhnlichen Benutzer immer "nein". Beim Typ zip 5.12 kann der Benutzer zwar keine Dateien importieren, gegebenenfalls kann jedoch ein Systemupdate durchgeführt werden (siehe unten). Bei Audio und Videodateien gelten die Kriterien der zugehörigen Objektklassenknoten 5.14 bzw. 5.15, das heißt sie können abgespielt werden, wobei Videodateien dem Benutzer nur für den Zugriff mit einer zugelassenen Applikation angeboten werden.

[0131] Bei unbekannten Objektklassen wird der Import direkt im CD-Ereignisknoten 5.3 abgelehnt, falls der Benutzer nicht der Administrator xy ist. Die entsprechende Verarbeitungsvorschrift wurde von der Wurzel 5.1 geerbt.

[0132] Will nun der Benutzer zum Beispiel mit einem Dateimanager auf den Inhalt der CD zugreifen, werden ihm von dem Dateimanager nur die importierbaren Dateien und Verzeichnisse angeboten.

[0133] Im weiteren wird ein Beispiel für ein Update des Zugriffsschutzsystems beschrieben.

[0134] Das Zugriffsschutzsystem kann verwendet werden um die eigene ACDB zu aktualisieren und auch um neue oder aktualisierte Proxies zu installieren. Beispielsweise können auf diese Art und Weise Hashwerte von neu zur Verwendung freigegebenen CDs in die ACDB eingetragen werden, es können also (auch über ftp) CDs in sicherer Weise freigegeben oder gesperrt werden, auch solche, die nicht von der administrierenden Stelle selbst ausgegeben werden.

[0135] Legt der Benutzer eine CD ein, welche eine Datei mit dem Namen acupdate.zip enthält, so wird wie im letzten Punkt beschrieben auf den Objektklassenknoten ZIP (5.12) verzweigt. Diese Datei kann auch über ftp (automatisch oder durch Benutzeraktion) in das Notebook gelangen, der zugehörige Ereignisknoten (5.5) erlaubt dies. In diesem Fall wird sie zunächst in einem dem Benutzer nicht zugänglichen Sicherheitsbereich importiert (4.20). Es wird nun untersucht, ob der Inhalt die gültige Unterschrift einer berechtigten Stelle trägt. Ist dies der Fall so wird automatisch die Datei entpackt und ein Systemupdate durchgeführt.

[0136] Im Folgenden wird nun ein Beispiel für ein Installieren freigegebener Software über CD beschrieben

[0137] Bei Einlegen der entsprechenden CD wird wieder auf den Objektklassenknoten CD-Inhalt (5.10) verzweigt. Der CD-Inhalt trägt jedoch eine Unterschrift, die vom Proxy überprüft werden kann. Ist es die korrekte Unterschrift einer berechtigten Stelle, so wird die CD zum Import in den Sicherheitsbereich freigegeben. Das immer auf einer solchen CD enthaltene Programm setup.exe wird unter Administratorrechten ausgeführt und installiert die auf der CD enthaltene Software mit einer definierten Konfiguration, die entweder auf der CD selbst oder in der ACDB enthalten sein kann.

[0138] In einem weiteren Ausführungsbeispiel kann Programm bereitgestellt sein, mit Instruktionen zum Ausführen der vorhergehend beschriebenen Schritte. Weiter kann ein Computer lesbares Medium bereitgestellt sein, in dem ein Programm verkörpert ist, wobei das Programm einen Computer anweist, die vorhergehend beschriebenen Schritte auszuführen. Ein Computerprogrammprodukt kann das Computer lesbare Medium umfassen.

[0139] Im Folgenden werden weitere Beispiele einiger Begriffe und Elemente der Beschreibung erläutert. Es wird darauf hingewiesen, dass die jeweiligen Erläuterungen lediglich weitere Beispiele darstellen und nicht als beschränkend auszulegen sind.

DV-Gerät: ein Hardware-Element oder eine Ansammlung von Hardware-Elementen (z. B. ein oder ein Intranet), in welchem definierte Schnittstellen zur Kommunikation existieren.

Benutzer: Ein Benutzer kann eine Person oder ein Programm sein, der/dem durch Betriebssystemmittel Zugriff auf Teile des DV-Gerätes gewährt ist.

Objekte: Objekte sind elementare Objekte oder Container. Elementare Daten: digitale Daten oder Objekte der realen Welt, deren Existenz und Semantik in digitale Daten abgebildet werden kann.

Digitale Daten: Dateien in elektronischer Form mit beliebigem Inhalt und Format oder digitale Datenströme. Dies können auch aktive Elemente sein, beispielsweise Programme, die Aktionen auf einem DV-Gerät auslösen können.

Container: Zusammenfassungen von elementaren Daten (z. B. Dateiverzeichnisse oder der vollständige Inhalt einer CD oder ein Bündel Geldscheine)

Objektklassen: Die Zugehörigkeit eines Objektes zu einer Klasse wird definiert durch Attribute und Qualitäten, die einem Objekt zugeordnet werden können, wie z. B. Dateixtensions, Dateinamen oder digitale Unterschriften.

Objektinstanz: konkrete Ausprägung einer Objektklasse.

Datenkanal: Schnittstelle, über welche Objekte in ein DV-Gerät eintreten oder es verlassen.

Ereignis: Handhabungsanweisung für Objekte oder ein Übertragungsversuch über einen realen oder virtuellen Datenkanal.

#### Patentansprüche

1. Verfahren zur Verarbeitungskontrolle von Objekten, mit den Schritten:

Erzeugen einer Kontrollanfrage durch eine Zugriffsvorrichtung bei Erfassung eines Ereignisses in Zusammenhang mit einem Objekt, wobei die Kontrollanfrage das Ereignis beschreibende Ereignisinformation und das Objekt beschreibende Objektinformation enthält; Übertragen der Kontrollanfrage an eine Steuervorrichtung;

Auswählen einer Verarbeitungsvorschrift für das Objekt aufgrund der Ereignisinformation und Objektinformation aus einem Zugriffsinformationsspeicher, der dem Objekt und dem Ereignis zugeordnete Verarbei-

- tungsvorschriften speichert; und  
Verarbeiten des Objekts entsprechend der Verarbeitungsvorschrift.
2. Verfahren nach Anspruch 1, wobei das Ereignis eine Handhabungsanweisung oder eine Anweisung für einen Übertragungsversuch über einen realen oder virtuellen Datenkanal darstellt.
3. Verfahren nach Anspruch 2, wobei die Anweisung zur Übertragung des Objektes über den Datenkanal einen Import des Objektes in eine oder einen Export aus einer Datenverarbeitungsvorrichtung von/zu einem Peripheriegerät oder von/zu einem Netzwerk beinhaltet.
4. Verfahren nach mindestens einem der Ansprüche 2 und 3, wobei eine Vielzahl von Datenkanälen der Zugriffsvorrichtung zugeordnet ist.
5. Verfahren nach mindestens einem der Ansprüche 2-4, wobei die Objektinformation Information über ein Subjekt enthält, welches das Ereignis initiiert hat.
6. Verfahren nach mindestens einem der Ansprüche 1-5, wobei die Verarbeitungsvorschrift zumindest einen Schritt der folgenden Liste beinhaltet:
- Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal;
  - Freigabe des Imports mindestens eines Teils des Objektes und Zuordnen von lokal gültiger Zugriffsschutzinformation;
  - Freigabe des Imports mindestens eines Teils des Objektes in einen gesicherten Speicherbereich;
  - Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal und Auslösung von definierten Verarbeitungsschritten.
7. Verfahren nach mindestens einem der Ansprüche 1-6, wobei das Objekt in Beziehung steht zu der Zugriffsvorrichtung und/oder dem Zugriffsinformationsspeicher.
8. Verfahren nach mindestens einem der Ansprüche 1-7, wobei die Auswahl der Verarbeitungsvorschrift ein Überprüfen von Attributen und/oder nachprüfbar Qualitäten des Objektes beinhaltet.
9. Verfahren nach mindestens einem der Ansprüche 1-8, wobei die Auswahl der Verarbeitungsvorschrift eine Berücksichtigung der Rolle des Subjektes beinhaltet, welches das Ereignis initiiert hat.
10. Verfahren nach mindestens einem der Ansprüche 1-9, wobei der Zugriffsinformationsspeicher einen ersten Speicherbereich mit Ereignisinformation zu einer Vielzahl von Ereignissen und einen zweiten Speicherbereich mit Objektinformation zu einer Vielzahl von Objekten enthält.
11. Verfahren nach mindestens einem der Ansprüche 1-10, wobei die Ereignisinformation in einer Baumstruktur mit Ereignisknoten gespeichert ist, wobei jedes Ereignis einem Ereignisknoten zugeordnet ist, und die Objektinformation in einer Baumstruktur mit Objektklassenknoten gespeichert ist, wobei jeder Objektklasse ein Objektknoten zugeordnet ist.
12. Verfahren nach mindestens einem der Ansprüche 1-11, wobei die Objektinformation eine Objektklasse und eine Objektinstanz oder eine Menge von Objektinstanzen umfasst.
13. Verfahren nach mindestens einem der Ansprüche 1-12, wobei eine Verarbeitungsvorschrift eine Knotenverarbeitungsvorschrift oder eine Objektverarbeitungsvorschrift ist; einem Ereignisknoten eine Objektklassenliste mit  $n \geq 0$  Objektklassen und eine Knotenverarbeitungsvor-

- schrift zugeordnet sind, und den Objektknoten eine Knotenverarbeitungsvorschrift und Instanzlisten mit  $m \geq 0$  Listeneinträgen zugeordnet sind, wobei jeder Listeneintrag eine Instanz oder eine Instanzmenge und eine zugehörige Objektverarbeitungsvorschrift enthält; und
- die Objektverarbeitungsvorschrift eines Listeneintrags einer positiven Identifizierung zugeordnet ist, sowie die Knotenverarbeitungsvorschrift eines Ereignisknotens und die Knotenverarbeitungsvorschrift eines Objektknotens einer negativen Identifizierung.
14. Verfahren nach mindestens einem der Ansprüche 11-13, wobei das Auswählen der Verarbeitungsvorschrift beinhaltet:
- Identifizieren des Ereignisknotens, dem der Ereignis zugeordnet ist;
- Suchen in der Objektklassenliste des identifizierten Ereignisknotens nach einer Objektklasse, die das Objekt umfasst; und
- Verarbeiten des Objektes gemäß der Knotenverarbeitungsvorschrift, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, nicht enthalten ist.
15. Verfahren nach mindestens einem der Ansprüche 1 und 14, wobei die Verarbeitungsvorschrift eine positive und eine negative Teilverarbeitungsvorschrift umfasst; und bei Erfüllung eines Ereigniskriteriums das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift verarbeitet wird und bei Nichterfüllung des Ereigniskriteriums das Objekt gemäß der negativen Knotenteilverarbeitungsvorschrift verarbeitet wird.
16. Verfahren nach Anspruch 15, wobei das Ereigniskriterium mindestens ein Element der folgenden Liste betreffen kann:
- einen zulässigen und gültigen Objektnamen;
  - einen gültigen Hashwert;
  - Information über den Initiator der Objektanfrage;
  - eine gültige und zulässige digitale Unterschrift;
  - eine Verschlüsselung; und
  - Referenzen auf notwendige Information.
17. Verfahren nach mindestens einem der Ansprüche 13-16, einschließlich, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, enthalten ist:
- Identifizieren des zugehörigen Objektklassenknotens;
- Suchen in der Instanzliste des identifizierten Objektklassenknotens nach einer Instanz, der die Instanz des Objektes entspricht;
- Auswahl der Objektverarbeitungsvorschrift, welche diesem Instanzlisteneintrag zugeordnet ist;
- Verarbeitung des Objektes gemäß dieser Objektverarbeitungsvorschrift, falls eine solche gefunden wurde; und
- Verarbeitung des Objektes gemäß der Knotenverarbeitungsvorschrift des identifizierten Objektklassenknotens, falls das Objekt in der Instanzliste nicht gefunden wurde.
18. Verfahren nach mindestens einem der Ansprüche 13-17, wobei die Knotenverarbeitungsvorschrift eines Objektknotens eine positive und negative Knotenteilverarbeitungsvorschrift umfasst und, falls in der Instanzliste keine dem Objekt entsprechende Instanz gefunden wurde, bei Erfüllung eines Objektknotenkriteriums das Objekt gemäß der positiven Knotenteilverarbeitungsvorschrift verarbeitet wird und bei Nichterfüllung des Objektknotenkriteriums das Objekt gemäß

der negativen Knotenteilverarbeitungsvorschrift verarbeitet wird.

19. Verfahren nach mindestens einem der Ansprüche 13–18, wobei die Objektverarbeitungsvorschriften eines Objektknotens positive und negative Objektteilverarbeitungsvorschriften umfassen, und wobei, falls in der Instanzliste des identifizierten Objektknotens eine dem Objekt entsprechende Instanz gefunden wurde und ein diesem Listeneintrag zugeordnetes Objektkriterium erfüllt ist, das Objekt gemäß der positiven Objektteilverarbeitungsvorschrift verarbeitet wird und bei Nichterfüllung des Objektkriteriums das Objekt gemäß der negativen Objektteilverarbeitungsvorschrift verarbeitet wird.
20. Verfahren nach mindestens einem der Ansprüche 1–19, wobei im Falle einer Containerinstanz die Verarbeitungsvorschrift aus der Anweisung besteht, die Zugriffentscheidung auf die Inhalte des Containers zu beziehen.
21. Verfahren nach mindestens einem der Ansprüche 1–20, wobei die Verarbeitungskontrolle verwendet wird, um Aktualisierungen in der Steuervorrichtung und/oder im Zugriffsinformationsspeicher vorzunehmen.
22. Ein Programm mit Instruktionen zum Ausführen des Verfahrens nach mindestens einem der vorhergehenden Ansprüche.
23. Ein Computer lesbares Medium, in dem ein Programm verkörpert ist, wobei das Programm einen Computer anweist, das Verfahren nach mindestens einem der Ansprüche 1–21 auszuführen.
24. Ein Computerprogrammprodukt, das Computer lesbare Medium nach Ansp
25. Vorrichtung zur Verarbeitungskontrolle von Objekten, umfassend:
  - eine Zugriffsvorrichtung, um eine Kontrollanfrage bei Erfassung eines Ereignisses in Zusammenhang mit einem Objekt zu erzeugen, wobei die Kontrollanfrage das Ereignis beschreibende Ereignisinformation und das Objekt beschreibende Objektinformation enthält; einen Zugriffsinformationsspeicher, um dem Objekt und dem Datenkanal zugeordnete Verarbeitungsvorschriften zu Speichern; und
  - eine Steuervorrichtung, um die Kontrollanfrage zu empfangen und aufgrund der Ereignisinformation und Objektinformation eine Verarbeitungsvorschrift für das Objekt auszuwählen und um eine Verarbeitung des Objekts entsprechend der Verarbeitungsvorschrift zu bewirken.
26. Vorrichtung nach Anspruch 25, wobei die Datenkanäle Verbindungen zu Peripheriegeräten einer Datenverarbeitungsvorrichtung darstellen.
27. Vorrichtung nach mindestens einem der Ansprüche 25 und 26, wobei die Datenkanäle Verbindungen zu oder externen Vorrichtungen in einem Netzwerk darstellen.
28. Vorrichtung nach mindestens einem der Ansprüche 25–27, wobei das Ereignis eine Handhabungsanweisung oder eine Anweisung für einen Übertragungsversuch über einen realen oder virtuellen Datenkanal darstellt.
29. Vorrichtung nach Anspruch 28, wobei die Anweisung zur Übertragung des Objektes über den Datenkanal einen Import des Objektes in eine oder einen Export aus einer Datenverarbeitungsvorrichtung von/zu einem Peripheriegerät oder von/zu einem Netzwerk beinhaltet.
30. Vorrichtung nach mindestens einem der Ansprü-

che 25–29, eine Vielzahl von Datenkanälen umfassend, die der Zugriffsvorrichtung zugeordnet ist.

31. Vorrichtung nach mindestens einem der Ansprüche 25–30, wobei die Objektinformation Information über ein Subjekt enthält, welches das Ereignis initiiert hat.
32. Vorrichtung nach mindestens einem der Ansprüche 25–31, mit einer Vorrichtung zur Veranlassung, in Übereinstimmung mit der Verarbeitungsvorschrift, zumindest eines Schrittes der folgenden Liste:
  - Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal;
  - Freigabe des Imports mindestens eines Teils des Objektes und Zuordnen von lokal gültiger Zugriffsschutzinformation;
  - Freigabe des Imports mindestens eines Teils des Objektes in einen gesicherten Speicherbereich;
  - Freigabe oder Sperrung der Übertragung des Objektes über einen Datenkanal und Auslösung von definierten Verarbeitungsschritten.
33. Vorrichtung nach mindestens einem der Ansprüche 25–32, wobei das Objekt in Beziehung steht zu der Zugriffsvorrichtung und/oder dem Zugriffsinformationsspeicher.
34. Vorrichtung nach mindestens einem der Ansprüche 25–33, mit einer Vorrichtung zur Überprüfung von Attributen und/oder nachprüfbaren Qualitäten des Objektes und einer dem entsprechenden Auswahl der Verarbeitungsvorschrift.
35. Vorrichtung nach mindestens einem der Ansprüche 25–34, mit einer Vorrichtung zur Berücksichtigung der Rolle des Subjektes, welches das Ereignis initiiert hat, und einer dem entsprechenden Auswahl der Verarbeitungsvorschrift.
36. Vorrichtung nach mindestens einem der Ansprüche 25–35, wobei der Zugriffsinformationsspeicher einen ersten Speicherbereich mit Ereignisinformation zu einer Vielzahl von Ereignissen und einen zweiten Speicherbereich mit Objektinformation zu einer Vielzahl von Objekten enthält.
37. Vorrichtung nach mindestens einem der Ansprüche 25–36, mit einer Baumstruktur mit Ereignisknoten, in der die Ereignisinformation gespeichert ist, wobei jedes Ereignis einem Ereignisknoten zugeordnet ist, und mit einer Baumstruktur mit Objektklassenknoten, in der die Objektinformation gespeichert ist, wobei jeder Objektklasse ein Objektklassenknoten zugeordnet ist.
38. Vorrichtung nach mindestens einem der Ansprüche 25–37, wobei die Objektinformation eine Objektklasse und eine Objektinstanz oder eine Menge von Objektinstanzen umfasst.
39. Vorrichtung nach mindestens einem der Ansprüche 25–38, wobei eine Verarbeitungsvorschrift eine Knotenverarbeitungsvorschrift oder eine Objektverarbeitungsvorschrift ist; einem Ereignisknoten eine Objektklassenliste mit  $n \geq 0$  Objektklassen und eine Knotenverarbeitungsvorschrift zugeordnet sind, und den Objektklassenknoten eine Knotenverarbeitungsvorschrift und Instanzlisten mit  $m \geq 0$  Listeneinträgen zugeordnet sind, wobei jeder Listeneintrag eine Instanz oder eine Instanzmenge und eine zugehörige Objektverarbeitungsvorschrift enthält; und die Objektverarbeitungsvorschrift eines Listeneintrags einer positiven Identifizierung zugeordnet ist, sowie

die Knotenverarbeitungsvorschrift eines Ereignisknotens und die Knotenverarbeitungsvorschrift eines Objektklassenknotens einer negativen Identifizierung.

40. Vorrichtung nach mindestens einem der Ansprüche 37–39, wobei das Auswählen der Verarbeitungsvorschrift beinhaltet:

Identifizieren des Ereignisknotens, dem das Ereignis zugeordnet ist;

Suchen in der Objektklassenliste des identifizierten Ereignisknotens nach einer Objektklasse, die das Objekt umfasst; und

wobei die Steuervorrichtung dazu ausgebildet ist, die Verarbeitung des Objektes gemäß der Knotenverarbeitungsvorschrift zu bewirken, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, nicht enthalten ist.

41. Vorrichtung nach mindestens einem der Ansprüche 25–40, wobei

die Verarbeitungsvorschrift eine positive und eine negative Teilverarbeitungsvorschrift umfasst; und

die Steuervorrichtung dazu ausgebildet ist, bei Erfüllung eines Ereigniskriteriums die Verarbeitung des Objekts gemäß der positiven Teilverarbeitungsvorschrift zu bewirken und bei Nichterfüllung des Ereigniskriteriums die Verarbeitung des Objekts gemäß der negativen Teilverarbeitungsvorschrift zu bewirken.

42. Vorrichtung nach Anspruch 41, wobei das Ereigniskriterium mindestens ein Element der folgenden Liste betreffen kann:

- einen zulässigen und gültigen Objektnamen;
- einen gültigen Hashwert;
- Information über den Initiator der Objektanfrage;
- eine gültige und zulässige digitale Unterschrift;
- eine Verschlüsselung; und
- Referenzen auf notwendige Informationen.

43. Vorrichtung nach mindestens einem der Ansprüche 39–42, wobei die Steuervorrichtung dazu ausgebildet ist, falls in der Objektklassenliste des identifizierten Ereignisknotens eine Objektklasse, die das Objekt umfasst, enthalten ist:

Identifizieren des zugehörigen Objektklassenknotens;

Suchen in der Instanzenliste des identifizierten Objektklassenknotens nach einer Instanz, der die Instanz des Objektes entspricht;

Auswahl der Objektverarbeitungsvorschrift, welche diesem Instanzlisteneintrag zugeordnet ist;

Verarbeitung des Objektes gemäß dieser Objektverarbeitungsvorschrift, falls eine solche gefunden wurde; und

Verarbeitung des Objekts gemäß der Knotenverarbeitungsvorschrift des identifizierten Objektklassenknotens, falls das Objekt in der Instanzliste nicht gefunden wurde.

44. Vorrichtung nach mindestens einem der Ansprüche 39–43, wobei die Knotenverarbeitungsvorschrift eines Objektklassenknotens eine positive und negative Knotenteilverarbeitungsvorschrift umfasst und die Steuervorrichtung dazu ausgebildet ist, falls in der Instanzliste keine dem Objekt entsprechende Instanz gefunden wurde, bei Erfüllung eines Objektklassenknotenkriteriums die Verarbeitung des Objekts gemäß der positiven Knotenteilverarbeitungsvorschrift zu bewirken und bei Nichterfüllung des Objektklassenknotenkriteriums die Verarbeitung des Objekts gemäß der negativen Knotenteilverarbeitungsvorschrift zu bewirken.

45. Vorrichtung nach mindestens einem der Ansprü-

che 39–44, wobei die Objektverarbeitungsvorschriften eines Objektklassenknotens positive und negative Objektteilverarbeitungsvorschriften umfassen, und die Steuervorrichtung dazu ausgebildet ist, falls in der Instanzliste des identifizierten Objektklassenknotens eine dem Objekt entsprechende Instanz gefunden wurde und ein diesem Listeneintrag zugeordnetes Objektkriterium erfüllt ist, die Verarbeitung des Objekts gemäß der positiven Objektteilverarbeitungsvorschrift zu bewirken und bei Nichterfüllung des Objektkriteriums die Verarbeitung des Objekts gemäß der negativen Objektteilverarbeitungsvorschrift zu bewirken.

46. Vorrichtung nach mindestens einem der Ansprüche 25–45, wobei im Falle einer Containerinstanz die Verarbeitungsvorschrift aus der Anweisung besteht, die Zugriffsentscheidung auf die Inhalte des Containers zu beziehen.

47. Vorrichtung nach mindestens einem der Ansprüche 25–46, wobei die Verarbeitungskontrolle verwendet wird, um Aktualisierungen in der Steuervorrichtung und/oder im Zugriffsinformationsspeicher vorzunehmen.

---

Hierzu 6 Seite(n) Zeichnungen

---

- Leerseite -

**THIS PAGE BLANK (USPTO)**

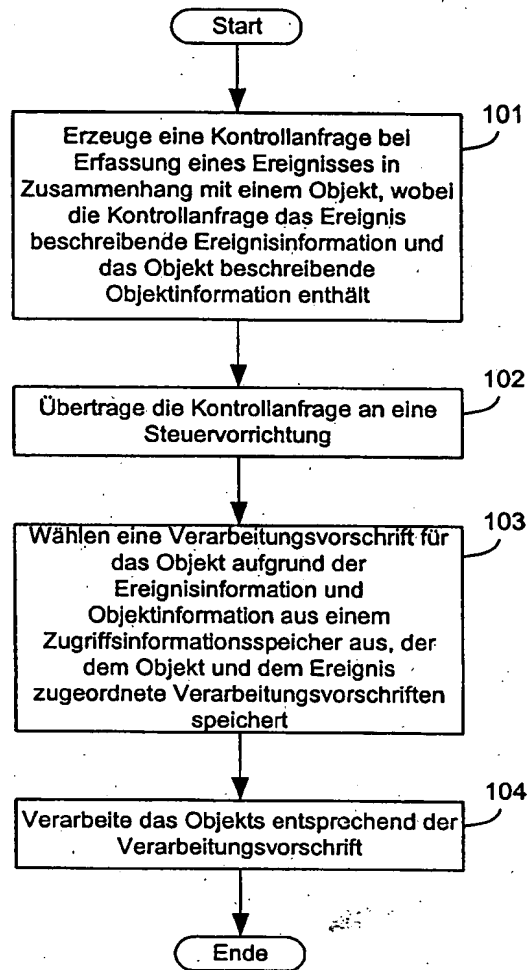


Fig. 1A

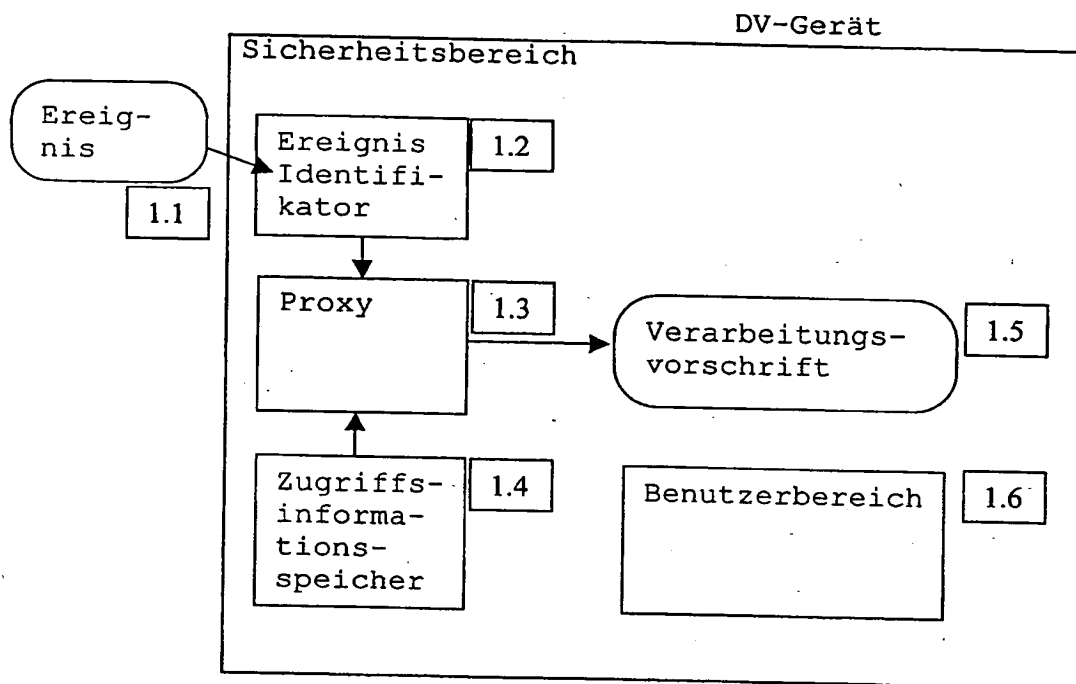


Fig. 1B

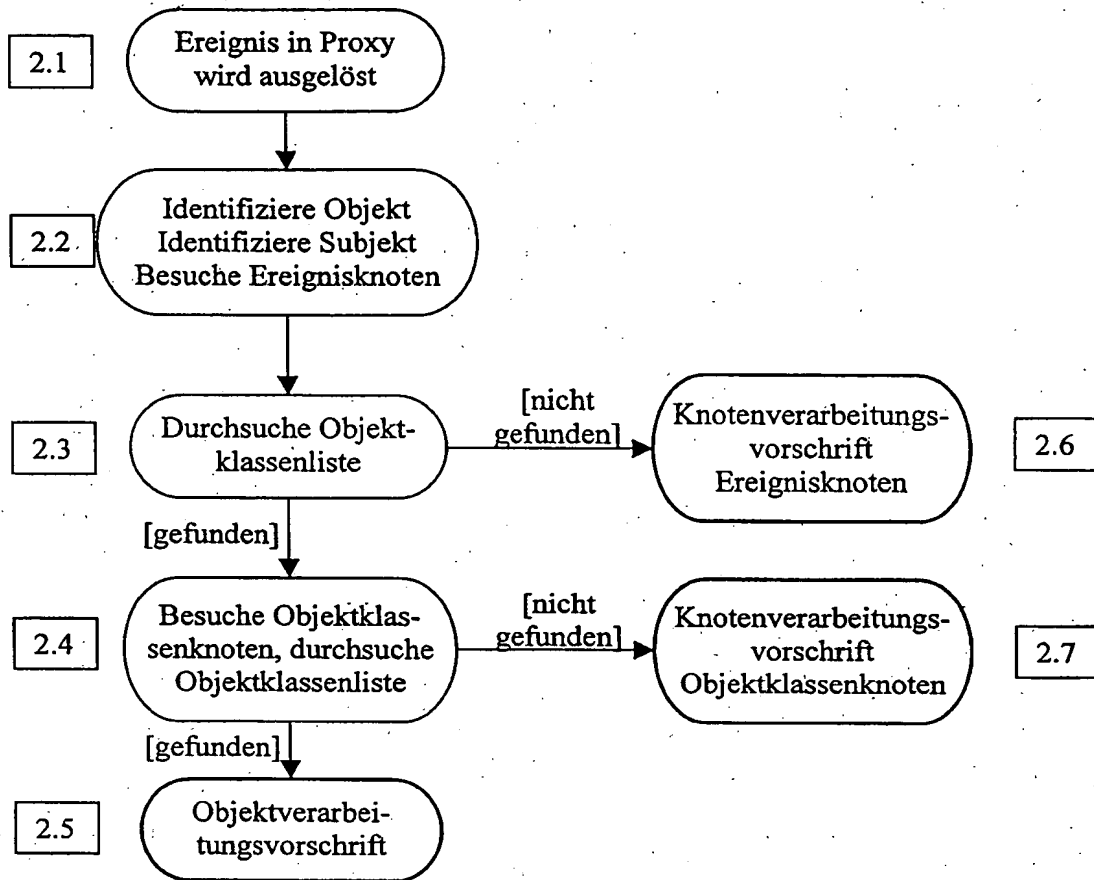


Fig. 2

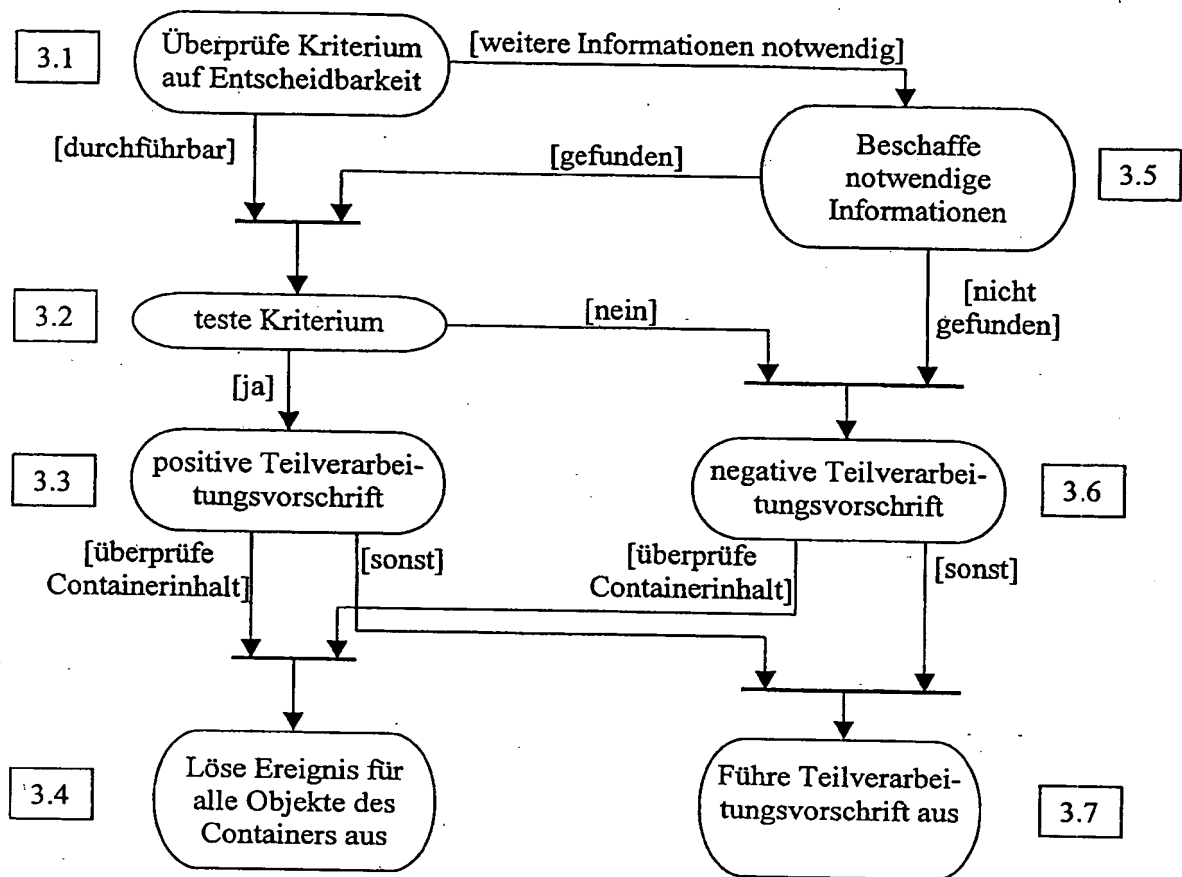


Fig. 3

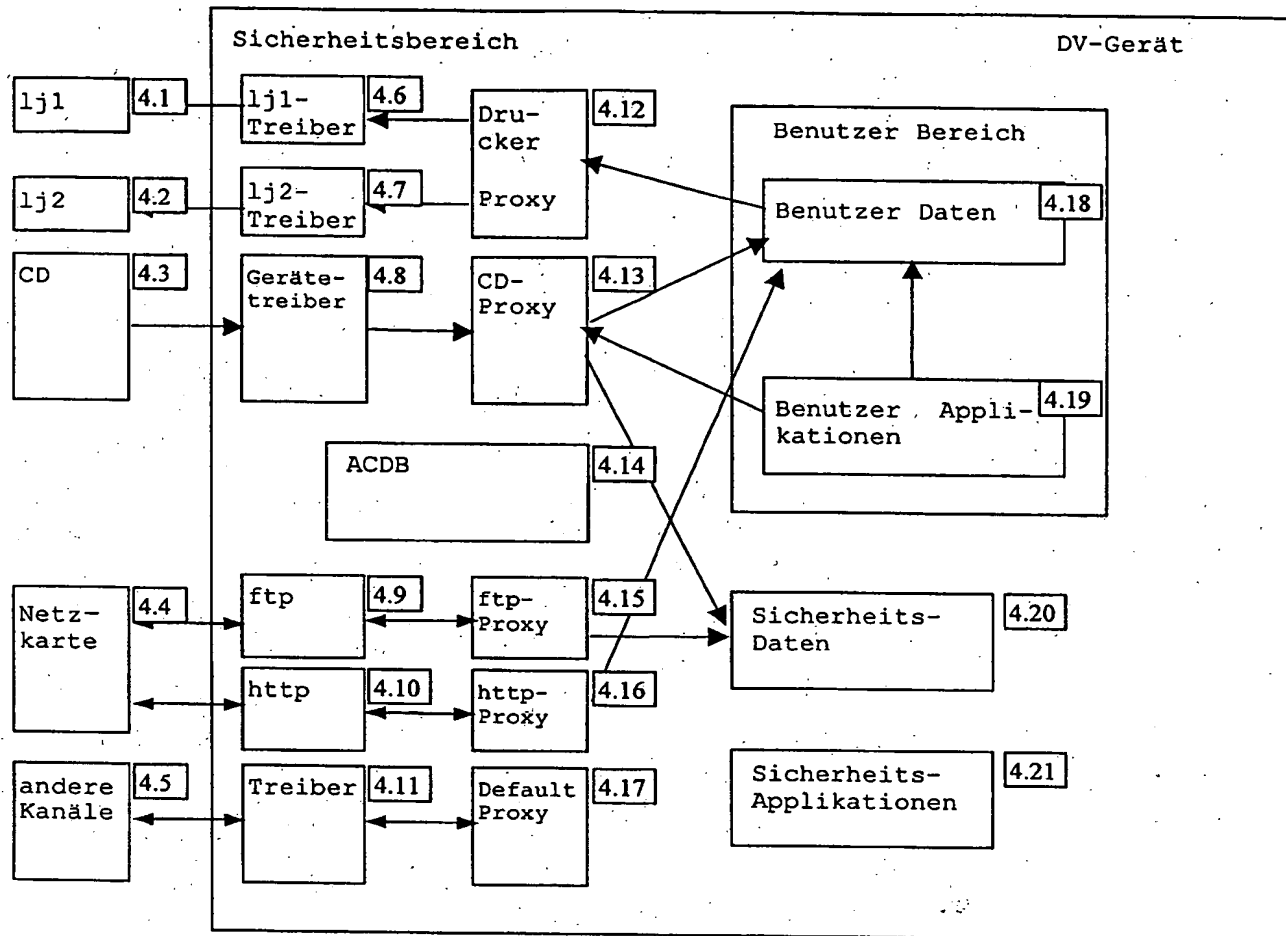
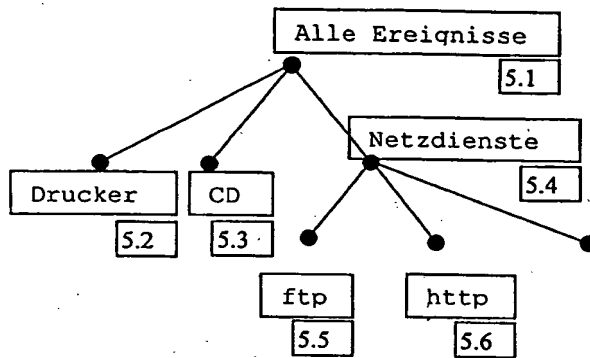


Fig. 4

Event Tree (ET)



Object Tree (OT)

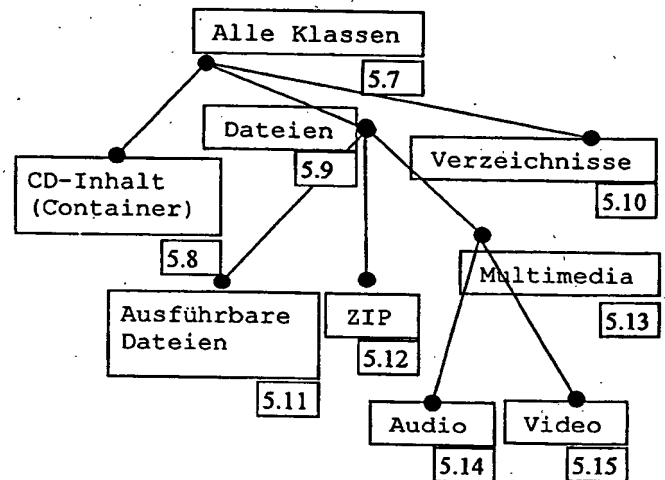


Fig. 5

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**